BY ORDER OF THE COMMANDER *AFSOC INSTRUCTION 33-302*
AIR FORCE SPECIAL OPERATIONS COMMAND *1 MARCH 1999*

Communication and Information

NATO CLASSIFIED HANDLING PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFSOC WWW site at: www.afsoc.af.mil/library. If you lack access, contact the OPR to obtain a copy.
OPR: HQ AFSOC/SCMN (TSgt Darryl Smaller)
Certified by: HQ AFSOC/SCMN (Ms. Mary L. Waxler)
Pages: 26
Distribution: F

This instruction implements AFPD 31-4, *Information Security Program* and AFI 31-401, *Information Security Program Management*. It is designed to provide you information concerning NATO classified handling requirements for Headquarters Air Force Special Operations Command and its subordinate units.

Page

Tables

Attachments

CHAPTER 1

NATO CLASSIFIED AUTHORITY

1.1. Introduction. The mission of AFSOC requires frequent access to NATO classified information, in garrison, TDY and at deployed sites. Access is based solely on "need to know" and should be scrutinized to validate individual access requirements. Individuals working in Operations and Intelligence are generally the primary users of NATO classified; however, other organizations may require this information for "operational" purposes when in performance of their duties. HQ AFSOC/SC manages the NATO Subregistry program for the command and provides specific guidelines and instructions that must be adhered to. All inquiries should be directed to HQ AFSOC/SCMN.

1.2. NATO Program Echelon. NATO classified documents originate only within those NATO alliance agencies authorized to develop them: HQ SHAPE, USECOM, AFCENT, AIRSOUTH etc., and other international countries currently part of the NATO alliance. Air Force activities not assigned within these agencies are not authorized to develop NATO classified documents.

1.2.1. Central US Registry (CUSR)**.** The Central US Registry, Pentagon, is the DOD single program manager for NATO classified handling and inquiries. Part of their duties include providing oversight and inspection of US facilities authorized to store and transmit NATO classified information, approving and disapproving request for establishment of NATO Subregistries and being the final US decision authority for NATO inquiries and use of information systems used for processing NATO classified.

1.2.2. Installation Information Security Office**.** The installation Security Forces, Information Protection office provides oversight and inspection, and investigates all security incidents involving NATO classified.

1.2.3. NATO Subregistry**.** Upon request from the organizational commander and with approval from the CUSR, NATO Subregistries are established to manage the NATO classified program for their base, there is only one subregistry on a base. The CUSR establishes the level of subregistries based on it's NATO classified holding. The current authorized holding level for the AFSOC NATO Subregistry is **NATO SECRET**. The NATO Subregistry Officer manages the NATO classified program their base or command, approves or disapproves unit commanders request for establishment of Control Points (CPs), and inspects those approved information systems used for processing NATO classified.

1.2.4. Control Points (CPs). Control Points are an extension of its parent subregistry; they control, distribute and destroy NATO classified documents for the unit or agency it supports. Unit commanders will appoint in writing at least two individuals as NATO Control Officers to manage their CP. These individuals will be the focal point for their unit day-to-day management of NATO classified. The level of the CP will not be higher than its subregistry.

1.2.5. User Offices**.** The office that uses the NATO classified to perform their mission. They protect, determined need-to-know access and is responsible for the destruction of NATO classified in their possession.

CHAPTER 2

PERSONNEL SECURITY REQUIREMENTS

2.1. Security Clearance Eligibility. Individuals requiring access to NATO classified information must have a final US security clearance eligibility at the equivalent level of the NATO classified material being given access.

2.2. Granting Access. NATO is a special access program requiring a briefing and formal access authorization before an individual is allowed access to NATO classified material. Commanders and staff agency chiefs are access granting authorities for NATO classified information under their control or supervision. The commander or staff agency chief need not have access in order to grant access for individuals under their control, they can delegate this authority to their deputies, executive officer, CPs officials or security managers. Indicate this delegation in writing to the NATO Subregistry Officer.

2.2.1. NATO Access for PCS Assignments**.** Individuals requiring NATO access for a PCS assignment, will be formally briefed into NATO at their new assignment. However, the individual will initiate all required paperwork for security clearance upgrade: TOP SECRET, SCI or periodic investigations prior to departure.

2.2.2. NATO Classified Briefings**.** Need-to-know is paramount in any granting of access to classified information. Commanders and staff agency chiefs should restrict access to those individuals who require access for mission accomplishment and monitor their continued need to that information. Attachment 3 contains the required information to be briefed for access to NATO classified. Access to NATO SECRET and below does not require a medical file review or Security Forces records check. The following are the NATO briefing requirements:

Table 2.1 NATO Classfied Briefing Requirements

CLASSIFIED LEVEL	INITIAL BRIEFING	DEBRIEFING	ANNUAL BRIEFING
ATOMAL (Any Level)	YES	YES	YES
COSMIC TOP SECRET (CTSA)	YES	YES	NO
NATO SECRET (NS)	YES	YES	NO
NATO CONFIDENTIAL (NC)	YES	YES	NO
NATO RESTRICTED (NR)	NO	NO	NO
NATO UNCLAS (NU)	NO	NO	NO

2.2.3. Documenting Access. Complete AF Form 2583, **Request for Personnel Security Action** as shown in attachment 5 to formally grant access to NATO classified. Retain a copy for the unit security manager files and forward a copy to the NATO Subregistry.

2.2.4. Terminating Access**.** A process should be in place to screen individuals with NATO access annually and during out-processing to ensure continued access requirement. When an individual's access to NATO is no longer needed, complete AF Form 2587**, Security Termination Statement**. Security managers will forward a copy to the NATO Subregistry Manager and retain their copy for two years.

Chapter 3

STORAGE, ACCOUNTABILITY AND CONTROL

3.1. Physical Security Requirements. The standards found in AFI 31-401 for the storage of US classified information are acceptable standards for comparable classification levels of NATO classified information. Store NATO classified material in:

3.1.1. A room or area continuously occupied by personnel with NATO access.

3.1.2. A secure storage room or vault approved for classified storage by 16th SFS/SFAI.

3.1.3. GSA approved security containers.

3.1.4 The above information is the minimal requirement; CPs and user office personnel must evaluate potential threats and provide additional protection if needed.

3.2. Storage Containers. Only those individuals who have been briefed into NATO are allowed access to safes containing NATO classified. Change safe combinations at least once a year, when personnel with access no longer require access, or when the combination is compromised. Record combination on SF 700, **Security Container Information** and post inside of safe.

3.2.1. Storage and Filing**.** NATO classified, except for ATOMAL, may be stored in the same security container with US classified as long as they are physically separated. Place a guide card between record groups in the container drawer or place the NATO classified documents in a separate drawer of a multi-drawer safe. Store all levels of NATO ATOMAL classified in a separate container from all other US and NATO classified material.

3.2.2. Classification Markings**.** Ensure NATO classified documents are marked with the appropriate classification; guide cards and folders are required to be marked to show the highest level of NATO classified contained.

3.3. Destruction. All classified destruction plans, to include emergency destruction, must include procedures for NATO classified. The NATO Subregistry will destroy all NATO ATOMAL and COSMIC TOP SECRET documents. NATO SECRET and below will be destroyed by two cleared individuals using AF Form 310, **Document Receipt and Destruction Certificate** or AF Form 145, **Certificate of Destruction of Material**, by the office maintaining the classified or as determined by the unit CP official when one exist. Forward a copy of AF Form 310 or 145 to the NATO Subregistry and maintained your copy for two years inactive. The following is the order of destruction of NATO classified when destroyed along with US classified:

Table 3.1 Classified Destruction Priority

SCI
COSMIC TOP SECRET ATOMAL
TOP SECRET
COSMIC TOP SECRET
SECRET
NATO SECRET
CONFIDENTIAL
NATO CONFIDENTIAL/RESTRICTED

3.4. Transmission. The most significant difference between US and NATO safeguarding standards is, that NATO uses a structured control system to transmit and account for NATO classified. The NATO Subregistry is the **ONLY** base agency authorized to receipt and dispatch NATO classified. The only current approved methods of transmission of NATO classified is by Defense Courier, US Registered Mail--NATO SECRET and below, and the Base Communications Centers (BCC). The NATO Subregistry may authorize CPs to receipt for NATO classified messages directly from the BCC. The following are guidelines for receiving and transporting NATO classified:

3.4.1. DO NOT transport NATO classified from or to ANY deployed or TDY location.

3.4.2. DO NOT transmit NATO classified over ANY communication network system. Exception: If you are at a NATO deployed or TDY location and that system has been approved for that purpose and you have been given permission by the host commander.

3.4.3. DO NOT discuss or turn over NATO classified to any person until verifying their access to NATO.

3.4.4. DO Notify the NATO Subregistry if NATO classified is sent to your office via Registered mail or hand carried.

3.4.5. Installation Transmission**.** NATO classified may be hand carried within the installation of the office having possession of the material for the purpose of attending meetings. Ensure

the appropriate classified cover sheet is used and classified is protected by a container to prevent disclosure of material.

3.5. Control of NATO Classified. NATO classified will be controlled using a chain of receipts, control logs and appropriate security measures consummate with the NATO classification maintained as indicated by this instruction.

3.6. Document Retention. Do not maintain NATO documents for historical purposes. CP officials and security managers will determined further need of NATO classified during their annual review of classified holdings to reduce levels needed for mission accomplishment. **NEVER** retire NATO classified to a records staging area.

3.6.1. NATO Classified Exercise Messages**.** No formal receipt or destruction control is required for exercise messages as long as they are destroyed within 30 days of exercise completion. Messages kept longer than thirty days will be formally controlled like all other messages.

3.7. Reproduction of NATO Classified. Limit reproduction of NATO classified to the minimum required for mission accomplishment. CPs and user offices may reproduce NATO SECRET and below documents under their control using the following guidelines:

3.7.1. Ensure copier used for reproduction has been cleared for the level of material being reproduced and area is secured. Security Managers are required to post a notice indicating this at the location of the copier.

3.7.2. Ensure individuals reproducing classified have been cleared for NATO classified.

3.7.3. Limit number of copies reproduced to the minimum needed for mission accomplishment.

3.7.4. Run at least two blank copies to clear the copier of any images that may be left on the drum. Completely sanitize the copier and work area to ensure that all classified have been removed.

3.7.5. CPs or user offices are responsible for ensuring the office they are providing copies of NATO classified to are have been cleared for NATO access, and understands the requirements of protecting NATO classified as determined by this instruction.

3.8. Administrative Controls. CPs or user office will assign control and copy numbers to each reproduced document. Example: DOO-98-001, Copy #1. This information will be placed visibly at the top of the document. Use a control log as shown in attachment 8 to further control these documents. CPs or user offices are responsible for supplying any updates to the original reproduced document to those offices that have a copy of the document. As you can see, a lot of controls must be provided to NATO classified. Before making the decision on coping NATO classified documents, determine the following:

3.8.1. Is the information being provided required for the office daily use?

3.8.2. How often will this information be required?

3.8.3. Can the requesting office review the material at the office maintaining the NATO classified information as needed?

3.8.4. Does the requesting office need to be on direct distribution?

3.9. NATO Classified Security Incidents. Notify the NATO Subregistry whenever there is a security incident involving NATO classified. All individuals appointed as inquiry or investigation officials will contact the NATO Subregistry manager prior to starting their duties and prior to out briefing the commander of the unit involved. Route all reports through the NATO Subregistry office for review prior to sending to the 16th SFS/SFAI, Information Protection Section. Attachment 4 contains more in-depth reporting procedures.

DOUGLAS R. COLEMAN, Colonel, USAF
Director, Communications and Information

Attachment 1

NATO CONTROL POINT APPOINTMENT LETTER

Figure A1. SAMPLE NATO CONTROL POINT APPOINTMENT LETTER

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPECIAL OPERATIONS COMMAND (AFSOC)

MEMORANDUM FOR HQ AFSOC/SCMN (NATO Subregistry)

FROM: 18th FLTS/CC

SUBJECT: Establishment of NATO Control Point (CP)

1. The following information is provided on our NATO Control Point.

    a. Location of CP: Bldg/Room #

b. Level of NATO CP: NATO SECRET

    c. Control Point hours of operation:

    d. This Control Point meets the requirements for storage of NATO SECRET material.

    e. The following individuals are appointed NATO CPs:

NAME	RANK	PHONE	SIGNATURE
NATO Control Officer:			
Grimes, Jeffrey	MAJ	4-2368	
Alternate(s):			
Baltimore, Walter	Capt	4-2368	

2. If there are any questions, POC is (must be a NATO CP official).

JACK JONES, Colonel, USAF
Commander

Attachment 2

NATO ACCESS GRANTING AUTHORITY

Figure A2. Sample NATO Access Approving Authority

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPECIAL OPERATIONS COMMAND (AFSOC)

MEMORANDUM FOR HQ AFSOC/SCMN (NATO Subregistry)

FROM: 18th FLTS/CC

SUBJECT: Authorization to Approve NATO Classified Access

1. The following individuals are authorized to approve access to NATO SECRET and below material:

NAME	RANK	PHONE	DUTY POSITION
Grimes, Jeffrey	Maj	4-2368	Operation Officer
Baltimore, Walter	Capt	4-2368	Security Manager
Miller, Albert	Capt	4-2109	Executive Officer

JACK JONES, Colonel, USAF
Commander

Attachment 3

NATO/ATOMAL ACCESS BRIEFING

A3.1. FOREWORD

A3.1.1. The following security briefing provides the minimum elements of information that must be provided to individuals upon initial indoctrination to NATO or/and ATOMAL access.

A3.1.2. This briefing is intentionally kept general in order to apply to all US Government users. Therefore, organizations are encouraged to expand upon these areas to specifically clarify internal procedures and policies. There are no requirements to maintain the same format or literary style; however, the minimum elements contained herein shall be included.

A3.2 INTRODUCTION

A3.2.1. In addition to access to U.S. classified material, the U.S. Government is placing special trust and responsibility in you by affording you access to NATO classified information. NATO is an abbreviation for the North Atlantic Treaty Organization.

A3.2.2. The Secretary of Defense is the United States Security Authority for NATO and is responsible for implementing NATO security requirements throughout the Executive Branch of the United States Government.

A3.2.3. NATO has four levels of classified material: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED, which are defined as follows:

A3.2.4. **COSMIC TOP SECRET (CTS)** -This security classification is applied to information or material the unauthorized disclosure of which would cause exceptionally grave damage to NATO. (NOTE: The marking "COSMIC" also is applied to TOP SECRET material that is the property of NATO. The term "NATO TOP SECRET" will not be used.

A3.2.5. **NATO SECRET (NS)** - This security classification is applied to information or material the unauthorized disclosure of which would cause grave damage to NATO.

A3.2.6. **NATO CONFIDENTIAL (NC)** - This security classification is applied to information or material the unauthorized disclosure of which would be damaging to the interests of NATO.

A3.2.7. **NATO RESTRICTED (NR)** - Is applied to information or material the unauthorized disclosure of which would be disadvantageous to the interests of NATO. (NOTE: Although the security safeguards for NATO RESTRICTED material is similar to those of FOR OFFICIAL USE ONLY, NATO RESTRICTED is still a security classification.)

A3.2.8. **NATO UNCLASSIFIED (NU)** - This marking is applied to information or material that is property of NATO, but does not require security protection.

A3.3. WHAT IS ATOMAL MATERIAL OR INFORMATION?

A3.3.1. ATOMAL information can be U.S. Restricted Data, Formerly Restricted Data, or United Kingdom Atomic information, which has been officially released to NATO.

A3.3.2. ATOMAL information is classified COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

A3.4. TO WHAT AM I AUTHORIZED ACCESS?

A3.4.1. NATO Classified Information. Your security official will inform you concerning your level of access to NATO classified material and whether you are authorized access to ATOMAL material (see below). Additionally, your organization/agency maintains a file or list indicating the levels of access for each individual assigned so that you can verify NATO access authorizations. As with U.S. material, access is NOT based on duty position, rank, or level of clearance. Access is based upon the proper level of U.S. clearance, the need-to-know and an access briefing to the specific level of NATO/ATOMAL authorized. Remember, IT IS YOUR RESPONSIBILITY to ensure that an individual is cleared and authorized access to that level of NATO classified or ATOMAL information BEFORE access is provided. If in doubt, seek assistance from your security, subregistry, or control point officials.

A3.4.2. A member of the Armed Forces or an employee of the Department of Defense or its contractors may be granted access to ATOMAL information once they have been cleared by the Department of Defense access to Restricted Data. An employee of NASA may be granted access to ATOMAL information concerning aeronautical and space activities only if the individual is cleared for such Restricted Data in accordance with Section 304 (b) of the National Aeronautics and Space Act of 1958, as amended, and subject to the requirement that there be a background investigation for access to ATOMAL information at the level of SECRET and above. All other individuals, and NASA employees requiring access to ATOMAL information other than that covering aeronautical and space matters, shall have a "Q" clearance issued by the Department of Energy in accordance with Section 145 of the Atomic Energy Act of *1954*, as amended. Interim clearances shall not be accepted as the basis for access to ATOMAL information.

A3.5. WHAT IS A REGISTRY SYSTEM?

A3.5.1. A Central Registry has been established by each NATO member nation to ensure proper control and accountability of NATO documents. The Central United States Registry (CUSR) is located in Room I B889, Pentagon, Washington DC. As an official representative of the U.S. Security Authority for NATO, the CUSR oversees the administration of the U.S. registry system. The CUSR establishes all U.S. subregistries to execute the operations of accountability and

security management of NATO and ATOMAL material at various U.S. locations throughout the world. Based on location and volume of material it may be necessary to further establish control points to assist in these operations.

A3.6. WHAT IS NATO MATERIAL OR INFORMATION?

A3.6.1. Material received from another NATO member nation may be either NATO or foreign government material. If the material has been marked "NATO" by the originating nation, it is NATO material and it is controlled under the NATO Security Program. If the document has only a classification marking and is not marked "NATO" by the originator, DO NOT mark the material NATO unless the originator informs you that the material is intended for NATO. You DO NOT have the authority to release that foreign government material into NATO.

A3.6.2. "RELEASABLE TO NATO" statements on U.S. originated material indicate that the material has been authorized under the National Disclosure Policy for release to NATO and may be discussed within the NATO community. However, ONLY the copies that are being released to NATO shall be marked "NATO" and controlled in the registry system. The remaining copies for U.S. use shall continue to be secured and controlled as U.S. material. There must be a record, however, that the material has been authorized for release to NATO.

A3.6.3. U.S. material containing NATO extracts shall be stored and controlled in accordance with Executive Order 12958 and agency implementing regulations. However, the material shall be marked to indicate that it contains NATO information.

A3.7. HOW DO I SAFEGUARD NATO AND ATOMAL MATERIAL?

A3.7.1. General. The physical security requirements for material marked NATO CONFIDENTIAL and above are the same as U.S. of the same level of classification. NATO RESTRICTED material may be stored in a filing cabinet, book case, desk or container in a room or building that is locked during non-duty hours, and access to the material is controlled. All personnel with access to a security container that is used to store NATO information must be authorized access to at least the level of the material that is intended for storage in that container.

A3.7.2. Segregation. You are required to ensure that all NATO and non-NATO material is filed separately. You are also required to file ATOMAL separately from non-ATOMAL material. This may be accomplished by separate safes, separate drawers or file dividers. Additionally, you are required to segregate ATOMAL control records from non-ATOMAL control records.

A3.7.3. Combinations. You are required to change combinations at least annually, upon departure of an individual with access to the combination, and if the combination has been or is suspected of having been compromised.

A3.7.4. Transmission. **The NATO Subregistry is the only agency authorized to transmit NATO classified.** The national or international transmission of CTS and CTSA material shall be through the registry system by a cleared government courier service, for example, diplomatic pouch or military courier service. The national transmission of NS, NSA, NC, and NCA shall be by cleared courier or by U.S. registered mail. In urgent situations, the United States Postal Service Express Mail may be used to transmit NS and below within the United States, its Territories, and the District of Columbia. The international transmission of NS, NSA, NC, and NCA shall be by a cleared U.S. government courier. In addition, NS, NSA, NC, and NCA material may be sent by U.S. Postal Service registered mail to an APO/FPO addressee. Finally, NR material may be sent by U.S. First Class mail within the United States and to an APO/FPO or NATO address through the U.S. or NATO member nation postal service.

A.3.7.5. Destruction. Destruction of CTS, CTSA, NS, NSA, and NCA material will be accomplished only by registry system personnel using a destruction certificate and a method approved for the destruction U.S. material of the same level of classification. Other NATO classified material may be destroyed by any means authorized for U.S. material of the same classification level.

A.3.7.6. Reproduction. Your security or registry system official will determine if you are authorized to reproduce NATO and/or ATOMAL information, and if so, explain to what classification levels, and the accountability and reporting requirements.

A.3.8. HOW DO I ACCOUNT FOR NATO AND ATOMAL MATERIAL?

A.3.8.1. You are required to maintain a receipt and logging system on the disposition and location of COSMIC TOP SECRET, NATO SECRET, and all ATOMAL material. In addition, each individual is required to execute a disclosure record upon acquiring access to CTS/CTSA material.

A.3.8.2. NATO CONFIDENTIAL and NATO RESTRICTED - You are required to maintain administrative control of NATO CONFIDENTIAL and NATO RESTRICTED material to preclude unauthorized access.

A.3.9. WHAT DO I DO IF I DISCOVER UNSECURED OR POSSIBLE LOST/COMPROMISED NATO CLASSIFIED MATERIAL?

A.3.9.1. General. The guidelines are very similar to those for U.S. material, except that your registry system and security officials also must be informed of the incident.

A.3.9.2. Procedures. If you find NATO/ATOMAL material unsecured and unattended, immediately contact your security and registry system officials. Stay with the material and wait for them to arrive. Do not disturb the area or material. Do not allow anyone else to disturb the area or allow uncleared or unauthorized personnel to have access to the material.

A.3.9.3. If it is absolutely required that you leave the area before your security or registry system official can take custody of the area; secure the material in the security container and lock the container. If the container is already locked or there is no container, take the material directly to the properly cleared and authorized security or registry system official.

A.3.9.4. Espionage, Sabotage, Terrorism, and Deliberate Compromise. Incidents involving a deliberate compromise of NATO/ATOMAL material, attempted or actual espionage directed against NATO/ATOMAL information, or actual or planned terrorist or sabotage activity against facilities or users of NATO/ATOMAL material, shall be reported promptly to the Federal Bureau of Investigation or your servicing counterintelligence representative (for military personnel).

A.3.9.5. Anyone with access to NATO/ATOMAL material could be a potential target. If you become aware of such incidents or someone approaches you directly to engage in such activities, remember the following:

A.3.9.5.1**. STAY CALM.** You are not at fault because they chose to target you.

A.3.9.5.2. **BE NONCOMMITTAL.** Do not commit yourself as to whether or not you will provide them with the material or information.

A.3.9.5.3. **REPORT IT PROMPTLY.** Even if it seems purely coincidental or insignificant, a small detail may be the key to solve a very important case. Do not discuss the incident with friends, family, co-workers, etc., unless directed to by your security official or counterintelligence representative.

A.3.9.5.4. **IT IS NEVER TOO LATE!** If you have provided material or information to an unauthorized recipient, REPORT IT. Do not continue to cause damage to U.S. and NATO security.

A.3.10. WILL NATO ACCESS LIMIT MY PERSONAL TRAVEL?

A.3.10.1. Your personal travel will not be limited based solely on the fact that you have access to NATO or/and ATOMAL information. However, travel to the countries whose political goals are not consistent with those of NATO is not advised. Check with your security representative for assistance. If you choose to travel to such countries, you are required to coordinate with your leave/travel order granting authority and security representative for a travel security briefing. Upon your return, your security representative will debrief you concerning your trip. At a minimum, you are required to report the following to your security representative: dates of the trip, countries visited, purpose of the trip, and if any incidents occurred, the circumstances and details.

ATTACHMENT 4

BREACHES OF SECURITY, AND LOSS OR COMPROMISE OF NATO CLASSIFIED INFORMATION

A.4. PURPOSE

A.4.1. The main purpose of investigating and reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever actions are necessary to minimize the damage.

A.4.2. DEFINITIONS

A.4.2.1. Breach of Security. A breach of security is an act, omission, or unauthorized deviation contrary to existing NATO security policy, or local security supplements, the results of which may endanger or subject NATO classified material to compromise.

A.4.2.2. Compromise. A compromise of NATO classified information exists if knowledge, either in whole or in part, passes to persons without authorized access to NATO classified information. A compromise is presumed if material has been subject to risk of unauthorized access when classified information is lost, even temporarily.

A.4.3. GENERAL

A.4.3.1. Any person who has knowledge of the actual or possible loss or compromise of NATO classified information or any other breach of security shall immediately report that knowledge to the appropriate security official as designated by organization heads.

A.4.3.2. Each breach of security shall be investigated to determine:

A.4.3.2.1. Whether NATO classified information has been compromised;

A.4.3.2.2. Whether any person who had or could have had access has at least some level of clearance, had been given a NATO classified briefing, and such individuals are of sufficient reliability and trustworthiness that no harm to NATO would result from the compromise.

A.4.3.2.3. Whether any remedial, corrective, disciplinary (including legal) action is recommended.

A.4.3.2.4. Investigations shall be conducted by a disinterested individual, E-7 and above, duly appointed by the organization head or designee. The investigating official shall have at least the equivalent level of clearance, be authorized access to at least the level of information concerned,

know the provisions of this instruction and, if possible, have an investigative or security background.

A.4.3.3. Compromise of NATO CRYPTO or COMSEC information shall be reported through the communications security channels instead of through Registry or USSAN channels.

A.4.4. INCIDENTS REPORTABLE TO THE FEDERAL BUREAU OF INVESTIGATION (FBI) OR APPROPRIATE COUNTERINTELLIGENCE OFFICE:

A.4.4.1. Attempts by unauthorized individuals to obtain classified or unclassified information concerning NATO facilities, activities, personnel, or material through questioning, elicitation, trickery, bribery, threats, or coercion, either through direct or indirect personal contacts or correspondence.

A.4.4.2. Attempts by unauthorized individuals to obtain NATO classified or unclassified information through photographing, wiretapping, eavesdropping, observing, or collecting material or information by any other means.

A.4.4.3. Attempts by individuals with known, suspected, or possible foreign intelligence backgrounds, associations or activities to establish any type of friendship, social or business relationships, or to place one under obligation through special treatment, favors, gifts, money, or other means.

A.4.4.4. Information concerning terrorist plans and activities posing a direct threat to NATO facilities, activities, personnel, or material.

A.4.4.5. Known or suspected acts or plots to harm or destroy NATO property by sabotage.

A.4.4.6. Known or suspected acts to deliberately compromise or disclose classified information to unauthorized individuals.

A.4.5. RESPONSIBILITIES:

A.4.5.1. The US Security Authority for NATO Affairs (USSAN) shall provide all initial and final reports to the NOS upon receipt of the appropriate information from the U.S. organizations.

A.4.5.2. The CUSR shall maintain a record of all compromise reports provided to the NOS by the USSAN, and monitor and enforce each reporting suspense.

A.4.5.3. The FBI shall keep the USSAN informed of all incidents concerning the actual suspected loss or compromise of NATO information, suspected/confirmed acts of sabotage, espionage, subversion, or terrorism directed toward NATO.

A.4.5.4. Organization heads or designees shall appoint investigating officers who shall ensure that investigations are thorough, timely, complete, and reported through channels to the USSAN.

A.4.5.5. All personnel, military or civilian, shall comply with the provisions of this Instruction and report any breaches of security or compromises to their appropriate security/counterintelligence officials.

A.6. PROCEDURES

A.6.1. Upon initial discovery of lost or missing CTS, NS or ATOMAL information, a preliminary inquiry shall be initiated and completed within five working days to determine if there has been a possible compromise. Organization heads or their appropriate designees shall provide an initial report to the USSAN, through their command NATO Subregistry Officer no later than 72 hours from the completion of the preliminary inquiry. The originator of the information shall be notified so that a damage assessment can be conducted. A final report shall be submitted by the investigating organization to the USSAN no later than 60 days from the initial report. The report shall be in compliance with the reporting format as stated below. If the 60-day suspense cannot be met, the USSAN shall be advised of the reason for the delay, the status of the investigation to date, and the date when the final report shall be provided.

A.6.2. An initial report to the USSAN is not required for those cases involving NC information unless there are any indications or suspicions of espionage. Final reporting procedures shall be the same as for COSMIC, NS and ATOMAL

A.6.3. An initial report to the USSAN is not required for those cases involving NR information unless there are any indications or suspicions of espionage. A copy of the final report, however, shall be available for review upon request during the annual inspections conducted by the CUSR.

A.7. REPORTING FORMAT

A.7.1. Initial reports shall contain the following information:

A.7.2. A description of the information involved, identified by NATO reference number/short title, classification, date, originator, unclassified subject and all copy numbers as applicable.

A.7.3. A brief description of the circumstances of the loss or compromise, including the dates or period(s) during which the material was not under control or the period(s) during which the information was subjected to compromise. Describe the number, clearance and any access authorization of the individuals who had unauthorized access.

A.7.4. Whether the originators have been notified and date of notification.

A.7.5. Final reports shall contain at least the following information:

A.7.6. A complete description of the circumstances concerning the discovery of the loss or possible compromise (include dates, times and locations). Explain any information that differs from the initial report. Provide the date and circumstances when the material was last under proper control and security accountability. If known, provide details of the disposition and degree of exposure of material to unauthorized persons until it was discovered missing or possibly compromised.

A.7.7. A complete description of the nature of the information involved, including whether the loss or unauthorized access was by oral, verbal, visual, or electronic disclosure. The description of the information involved shall include NATO reference number/short title, classification, serial and/or reproduced copy numbers, date, originator, and unclassified subject/title.

A.7.8. The estimated degree of compromise, with full justification of the conclusions reached. Conclusions that no compromise occurred during the period of time, that the material was out of authorized control, shall be fully supported by factual information.

A.7.9. The individual(s) by title or position, without name(s), upon whom the responsibility has been fixed. Specify the corrective and/or disciplinary action taken, if any;

A.7.10. An explanation of the cause of the loss or compromise (e.g., procedural, human error, equipment failure, etc.).

A.7.11. An explanation of countermeasures and corrective actions taken or contemplated to correct deficiencies and/or prevent recurrence. If such actions and countermeasures have not been completed by the time of the submission of this report, include a plan of action and estimated completion date.

A.7.12. Whether the originator was notified and dates of notification. Include a list of other organizations that were also notified.

A.8. CASE CLOSURE

A.8.1. The USSAN shall review the report and determine case closure. When the final report of investigation shows that accountable material has been irretrievably lost, the USSAN may grant release of the material from accountability.

A.8.2. Reports of investigations will remain on file at the unit for at least 3 years from closure.

A.9. COMPROMISES OF CRYPTOGRAPHIC MATERIAL

A.9.1. Compromises of NATO cryptographic material shall be reported through U.S. and NATO COMSEC channels.

Attachment 5

SAMPLE AF FORM 2583, REQUEST FOR PERSONNEL SECURITY ACTION

REQUEST FOR PERSONNEL SECURITY ACTION

AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101; and EO 9397.
PRINCIPAL PURPOSES: To identify investigation, security clearance, unescorted entry requirements, and special access program authorizations.
ROUTINE USES: To request personnel security investigations, record emergency or limited access authorization, entry to restricted areas, and to record special access program authorizations. SSN is used for positive identification of the individual and records.
DISCLOSURE IS VOLUNTARY: Failure to information and SSN could result in assignment to less sensitive duties.

I. IDENTIFYING INFORMATION

1. NAME (Last, First, Middle, Maiden)	2. ORGANIZATION OR FIRM SPONSOR
SMALLER, DARRYL	HQ AFSOC/SCMN

3. GRADE	4. SSN	5. CITIZENSHIP					
TSGT	000-00-0000	X	US CITIZEN		IMMIGRANT ALIEN		NON US NATIONAL

6. DATE OF BIRTH	7. PLACE OF BIRTH (City, State, and Country)
1 Jun 98	PHILADELPHIA PA

II. INVESTIGATION, CLEARANCE, ELIGIBILITY, ENTRY AND ACCESS REQUIREMENTS

8. INVESTIGATION REQUIREMENT		9. CLEARANCE, ENTRY OR ACCESS REQUIREMENT			
	NATIONAL AGENCY CHECK (NAC)		ONE-TIME ACCESS		LIMITED ACCESS
	NATIONAL AGENCY CHECK-WRITTEN INQUIRIES (NACI)		INTERIM CLEARANCE	X	SPECIAL ACCESS
	BACKGROUND INVESTIGATION (BI)		FINAL CLEARANCE		UNESCORTED ENTRY
	SPECIAL BACKGROUND INVESTIGATION (SBI)		TOP SECRET		PRIORITY A
	BI PERIODIC REINVESTIGATION (PR)		SECRET		PRIORITY B
	SBI PERIODIC REINVESTIGATION (PR)		CONFIDENTIAL		PRIORITY C

III. LOCAL FILES CHECK

10. TO:	11. FROM:
HQ AFSOC/CCQ	HQ AFSOC/SCP (Security Manager)

12. DATE	13. TYPED NAME, GRADE AND TITLE OF REQUESTER	14. SIGNATURE
25 Apr 98	SUSAN P. HYUNDAI, TSgt, USAF Security Manager	

IV. MEDICAL RECORDS CHECK

15. I CERTIFY a medical records check required by DOD 5200.2R/AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

16. DATE	17. TYPED NAME AND GRADE OF BASE DIRECTOR, MEDICAL SERVICES	18. SIGNATURE

V. SECURITY POLICE RECORDS CHECK

19. I CERTIFY a security police records check required by AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

20. DATE	21. TYPED NAME AND GRADE OF SECURITY POLICE OFFICIAL	22. SIGNATURE

VI. ACCESS AUTHORIZATION

ONE-TIME ACCESS		LIMITED ACCESS		CNWDI	X	NATO		SIOP-ESI	
						SECRET		CONTINUING	ONE-TIME

23. I CERTIFY the named individual requires access to the above special program(s), meets all investigative and clearance requirements, and has been briefed on program responsibilities as outlined in the governing directive. If applicable, emergency or limited access is necessary and will not endanger the national security.

24. DATE	25. TYPED NAME, GRADE AND TITLE OF APPROVING AUTHORITY	26. SIGNATURE
25 Apr 98	OLIVER BRYANT, Lt Col, USAF Chief, Mission Systems Division	

27. DATE	28. TYPED NAME, GRADE AND TITLE OF SPECIAL ACCESS PROGRAM CERTIFYING OFFICIAL	29. SIGNATURE
25 Apr 98	OLIVER BRYANT, Lt Col, USAF Chief, Mission Systems Division	

VII. REMARKS

30. *(If more space is needed, use reverse and show item number being continued)*
Individual briefed IAW AFSOCI 33-302 on _____
(Date and signature)

AF Form 2583, MAR 87 *(EF)* PREVIOUS EDITION WILL BE USED.

Attachment 6

SAMPLE AF FORM 2587, SECURITY TERMINATION STATEMENT

SECURITY TERMINATION STATEMENT

I am aware of my termination for access to NATO SECRET
(Enter special access being terminated, for example, "NATO Secret," or "SIOP-ESI," or enter special access being terminated and "classified information" if both are being terminated at the same time; otherwise, enter "classified information.") I acknowledge:

1. I have read and understand the below provisions of the Espionage Act *(18 U.S.C. 793, 794)*, the Atomic Energy Act *(42 U.S.C. 2274-2277)*, and the Subversive Activities Control Act of 1950, as amended *(50 U.S.C. 783)*. I understand that any unauthorized disclosure of information affecting the national defense is prohibited and punishable by law.

2. I do not have in my possession or control any documents or material of a classified nature.

3. I shall not knowingly or willfully divulge, reveal or transmit classified information orally or in writing or by any other means, to any unauthorized person or agency.

4. I shall report to the Federal Bureau of Investigation, to a security office of the Department of Defense, or to a security office of a U.S. Embassy or Consulate, without delay, any attempt made by an unauthorized person to solicit or obtain classified information.

5. I, have, have not *(Strike out inappropriate word or words)* received an oral security debriefing.

ESPIONAGE ACT AND OTHER CRIMINAL STATUTES

Sections 793 and 794 of Title 18, U.S. Code; Section 783 of Title 50, U.S. Code, and Sections 2274, 2275, 2278 and 2277 of Title 42, U.S. Code, identify and prescribe punishments for certain acts or the conspiracy to commit certain acts which one has reason to believe will injure the United States or secure an advantage to a foreign nation. These acts are:

1. Gathering, transmitting, delivering, communicating or disclosing information relating to national defense *(Including Restricted Data)* to an unauthorized person or causing these acts;

2. Losing information relating to national defense through gross negligence;

3. Failing to report to superiors the known loss or theft of information relating to national defense;

4. Communicating classified information to an agent or representative of a foreign government;

5. Failing to deliver on demand documents or information relating to the national defense to an officer or employee of the United States who is entitled to receive it; and

6. Gathering or delivering information relating to the national defense to aid a foreign government.

You have had access to information relating to the national defense *(Including Restricted Data)* which is protected by these statutes. These statutes make it a crime to unlawfully communicate information relating to the national defense to any person when there is reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign government. The penalties prescribed for violations of these statutes, through willful acts or gross negligence, vary according to the statute, the circumstances, and the information involved. They range in severity from a fine of not more than $2,500 to life imprisonment or death. Your signature on this form is your acknowledgement that you have been informed of the criminal statutes applicable to espionage and the punishments provided for violation of these statutes. The full text of the applicable section of each of these statutes is available for your review prior to signing this termination statement.

DATE	TYPED OR PRINTED NAME & GRADE OF PERSON BEING DEBRIEFED	SIGNATURE
25 Apr 98	DARRYL SMALLER, TSGT, USAF	
DATE	**TYPED OR PRINTED NAME OF DEBRIEFER**	**SIGNATURE**
25 Apr 98	MIKE SHURGART, CAPT, USAF Security Manager	

AF FORM 2587, SEP 91 *(EF)* PREVIOUS EDITION WILL BE USED.

Attachment 7

SAMPLE

AF FORM 310, DOCUMENT RECEIPT AND DESTRUCTION CERTIFICATE

DOCUMENT RECEIPT AND DESTRUCTION CERTIFICATE

1. TO: HQ AFSOC/SCMN (NATO Subregistry)	2. FROM: 18th FLTS/DO	3. DATE: 26 Apr 98 4. CONTAINER NO.

5. DESCRIPTION OF DOCUMENT(S): *(Indicate overall classification, originator, type (letter, message, plan, etc.), date, unclassified subject title, number of copies, and originator control number and copy number if Top Secret. Also use these data elements for identifying any attachments that would require a receipt if transmitted separately.)*

(NS) FIVEATAF MSG, 01000Z MAY 98, VOLENT PUSH 98 (NU),
1 CY,//
//LAST ITEM//

TO AVOID TRACER ACTION, RETURN SIGNED RECEIPT BY →	6. DATE

DOCUMENT RECEIPT

I ACKNOWLEDGE RECEIPT OF THE ABOVE DOCUMENTS

7. DATE RECEIVED	8. NAME, ORGANIZATION, AND PHONE NUMBER (DSN)	9. SIGNATURE OF RECIPIENT

DESTRUCTION CERTIFICATE

10. THE DOCUMENT(S) LISTED ABOVE WERE	X	DESTROYED		COMMITTED TO CENTRAL DESTRUCTION FACILITY ON →	11. DATE

12. TYPED OR PRINTED NAME AND SIGNATURE OF WITNESSING OFFICIAL	13. TYPED OR PRINTED NAME AND SIGNATURE OF WITNESSING OFFICIAL
JEFFREY GRIMES, MAJ, USAF	MIKE JONES, TSGT, USAF

AF FORM 310, NOV 95 *(EF-V1)* (PerFORM PRO) PREVIOUS EDITION WILL BE USED.

Attachment 8

SAMPLE AF FORM 145, CERTIFICATE OF DESTRUCTION OF MATERIAL

CERTIFICATE OF DESTRUCTION OF MATERIAL

INSTRUCTIONS

1. Under the heading "DESCRIPTION OF MATERIAL" list the classification, type of material (DIN, message, OPLAN, etc.) unclassified subject or title, office of origin, date and, when appropriate, any control number or other identifying data. In addition, either add separate, subordinate descriptions of endorsements and attachments, giving the above data for each, or list the number of endorsements and attachments.
2. After the final entry under "DESCRIPTION OF MATERIAL," type or draw a horizontal line and enter the words "Last Item."
3. In the signature blocks, enter the signature and grade of the officials executing the certificate.
4. Delete the inapplicable portions of items marked with an asterisk (*) below:
   a. The normal destruction procedure is used, delete the words "committed to the special destruction activity" and "CERTIFYING."
   b. The special destruction procedure is used, delete the words "destroyed" and "DESTROYING."

TO: (Office or unit to which the certificate must be furnished)	FROM: (Office or unit responsible for destroying the material or committing it to the special destruction activity)
HQ AFSOC/SCMN (NATO Subregistry)	18th FLTS/DOO

DESCRIPTION OF MATERIAL	DATE OF DOCUMENT	COPY NOS. (If any)	NUMBER OF COPIES
(NS) FIVEATAF MSG, 011000Z APR 98, VOLENT PUSH OP (NU) (NS) FIVEATAF MSG, 011096Z APR 98, VOLENT PUSH (NU)			

The material listed above has been *(destroyed) (committed to the special destruction activity) according to AFR 205-1. DATE

*(DESTROYING) (CERTIFYING) OFFICIAL	WITNESSING OFFICIAL
JEFFREY GRIMES, MAJ, USAF	MIKE JONES, TSGT, USAF

AF FORM 145, DEC 77 *(EF)* PREVIOUS EDITION WILL BE USED.

Attachment 9

SAMPLE AF FORM 3131, NATO CLASSIFIED REPRODUCTION CONTROL LOG

NATO CLASSIFIED REPRODUCTION CONTROL LOG

TYPE/SENDER/UNCLASS SUBJECT	UNIT CONTROL #	SENT TO	DATE SENT		
(NC) FIVEATAF MSG, 011000Z APR 98, MISSION SORTS (NU)	18th FLTS-98-001	4th SOS/IN	26 APR 98		

AF FORM 3131, MAY 83 *(EF)* PREVIOUS EDITION WILL BE USED. GENERAL PURPOSE *(11 x 8-1/2")*